ECE 297:11 - Lecture 1

Security Services

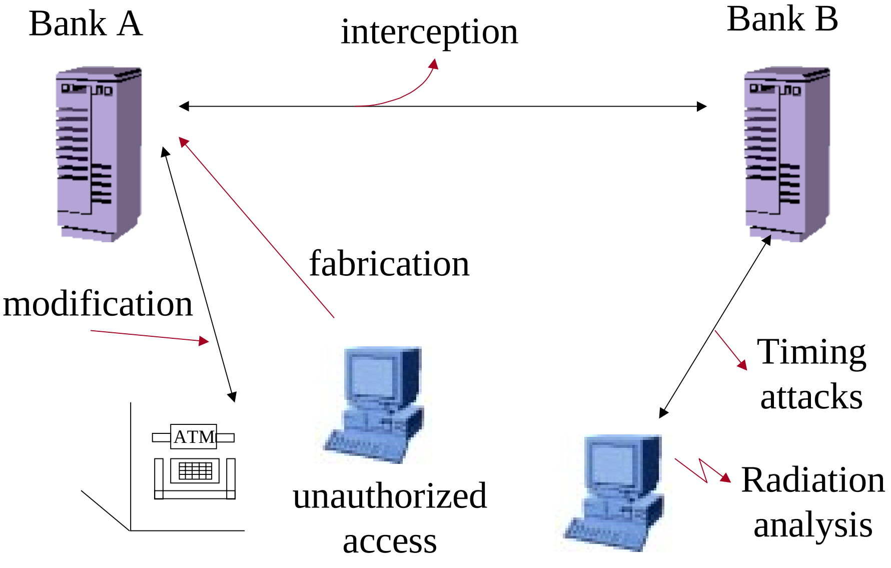
Basic Concepts of Cryptology

Need for *information security*

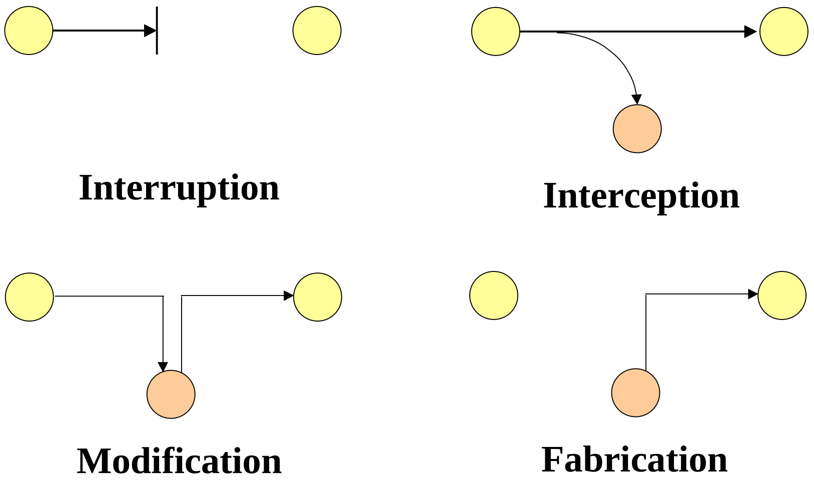
- widespread use of data processing equipment:
  computer security
- widespread use of computer networks and distributed computing systems:
  network security

Security Threats and Security Services

Security Threats in Banking Systems



Network Security Threats (1)



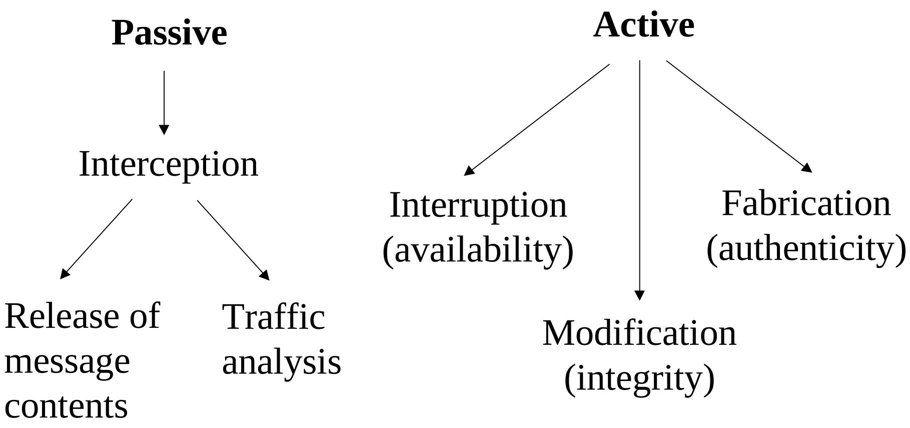
Interruption

Interception

Modification

Fabrication

Network Security Threats (2)



Passive

Interception

Release of message contents

Traffic analysis

Active

Interruption (availability)

Modification (integrity)

Fabrication (authenticity)

Security services

Protecting data

in transit

- **confidentiality**
- **integrity**
- **authentication**
- **non-repudiation**

at rest

- **access control**
  - **identification**
  - **authorization**
  - **auditing**
- **availability**

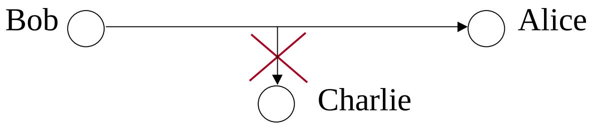
Identification
(User Authentication)

On the basis of

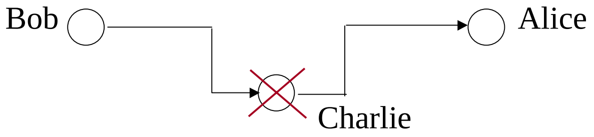
- **what you know** (passwords, PINs)
- **what you have** (magnetic card, smart card)
- **what you are** (fingerprints, handprints, voiceprints, keystroke timing, signatures, retinal scanners)

Basic Security Services (1)

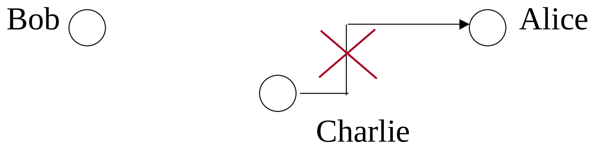
1. Confidentiality



2. Message integrity



3. Message authentication

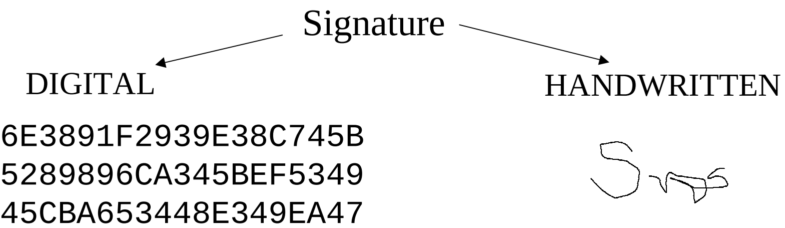


Basic Security Services (2)

4. Non-repudiation

- of sender - of receiver - mutual

Technique: *digital signature*



```
A6E3891F2939E38C745B
25289896CA345BEF5349
245CBA653448E349EA47
```

Main Goals:
- unique identification
- proof of agreement to the contents of the document

Handwritten and digital signatures

Common Features

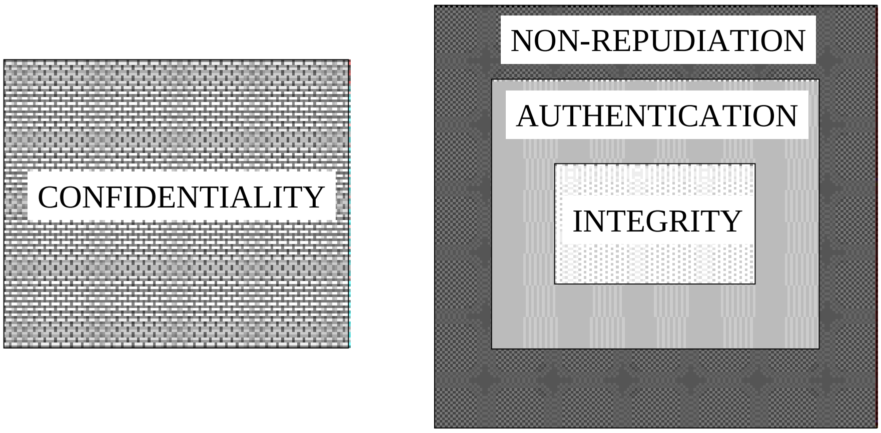
<table>
<tr><th>Handwritten signature</th><th>Digital signature</th></tr>
<tr><td colspan="2"><b>1. Unique</b>
<b>2. Impossible to be forged</b>
<b>3. Impossible to be denied by the author</b>
<b>4. Easy to verify by an independent judge</b>
<b>5. Easy to generate</b></td></tr>
</table>

Handwritten and digital signatures

Differences

Handwritten signature	**Digital signature**
6. Associated physically with the document	6. Can be stored and transmitted independently of the document
7. Almost identical for all documents	7. Function of the document
8. Usually at the last page	8. Covers the entire document

Relations among security services



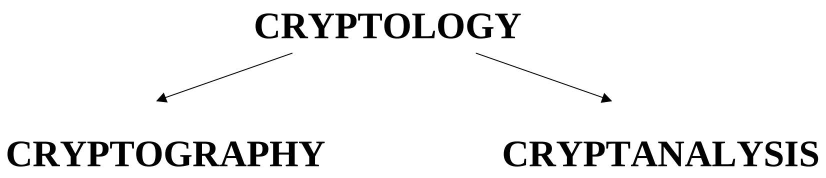
CONFIDENTIALITY

NON-REPUDIATION

AUTHENTICATION

INTEGRITY

Basic Concepts of Cryptology



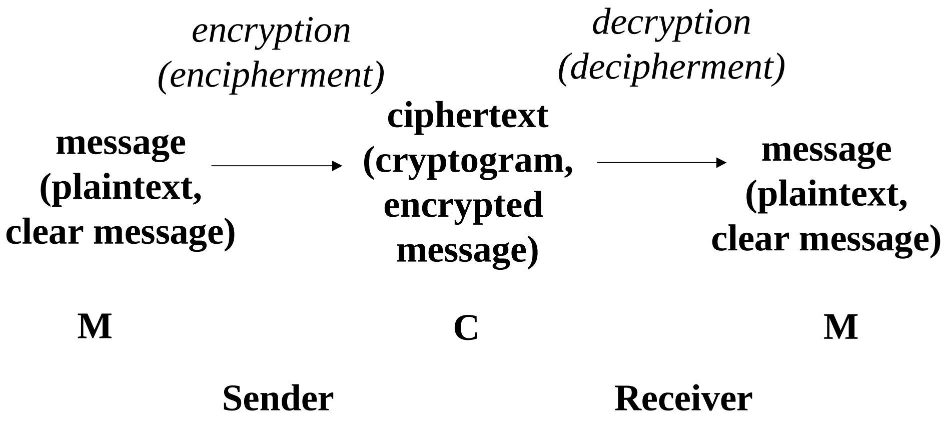
CRYPTOLOGY

CRYPTOGRAPHY **CRYPTANALYSIS**

from Greek

cryptos - hidden, secret
logos - word
graphos - writing

Basic Vocabulary



encryption
(encipherment)

decryption
(decipherment)

message
(plaintext,
clear message)

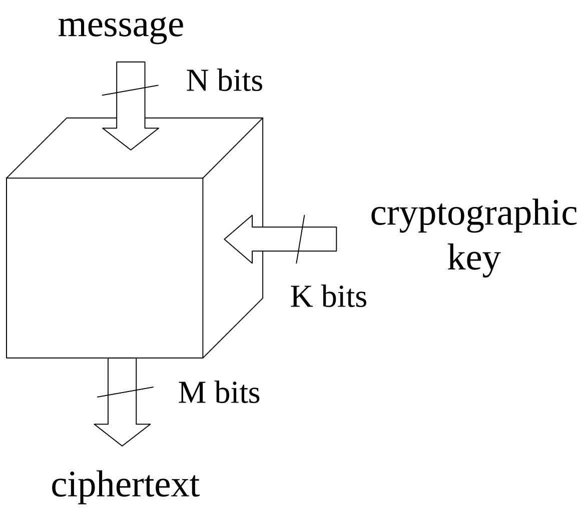
ciphertext
(cryptogram,
encrypted
message)

message
(plaintext,
clear message)

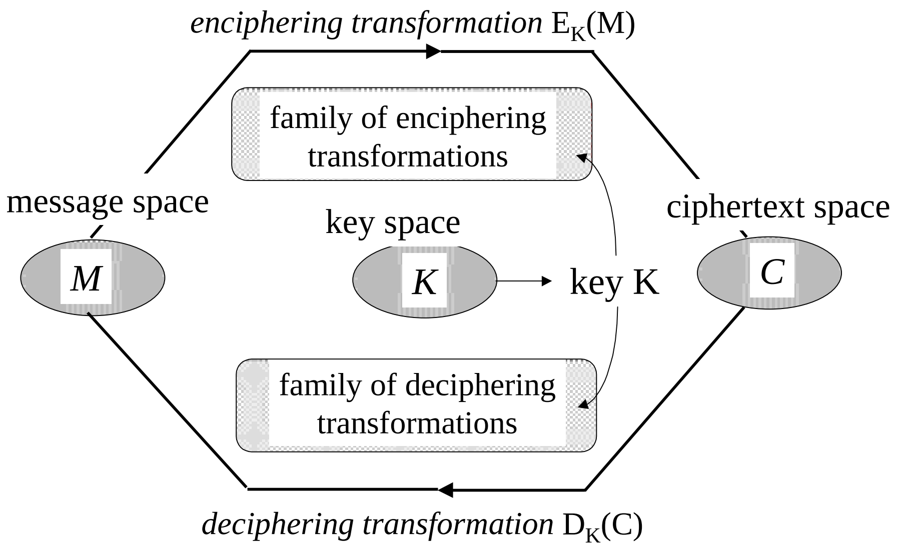
M **C** **M**

Sender **Receiver**

Cryptosystem (Cipher)



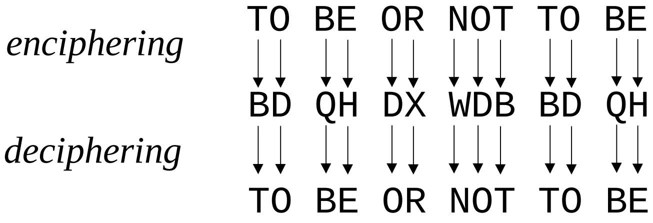
Definition of a cryptosystem (cipher)


enciphering transformation $E_K(M)$
family of enciphering transformations
message space
key space
ciphertext space
M
K
key K
C
family of deciphering transformations
deciphering transformation $D_K(C)$

$\forall\ K \in \mathit{K} \quad \forall\ M \in \mathit{M} \qquad D_K(E_K(M)) = M$

Substitution Cipher

$$\text{Key} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ f & q & i & s & h & n & c & v & j & t & y & a & u & w & d & r & e & x & l & b & m & z & o & g & k & p \end{pmatrix}$$



enciphering

```
TO BE OR NOT TO BE
BD QH DX WDB BD QH
```

deciphering

```
BD QH DX WDB BD QH
TO BE OR NOT TO BE
```

Number of keys = $26! \approx 4 \cdot 10^{26}$

Kerckhoff’s principle

The security of a cipher MUST NOT depend on anything that cannot be easily changed

A. Kerckhoff, 1883

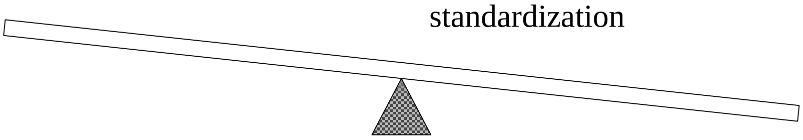
Unpublished vs. published algorithm?

Unpublished algorithm

1. Cryptanalysis must include recovering the algorithm
2. Smaller number of users, smaller motivation to break
3. Unavailable for other countries

Published algorithm

1. The only reliable way of assessing cipher security
2. Prevents backdoors hidden by designers
3. Large number of implementations = low cost + high performance
4. No need for anti-reverse-engineering protection
5. Software implementations
6. Domestic and international standardization



Fundamental Tenet of Cryptography

If lots of smart people have failed to solve a problem, then it probably will not be solved anytime soon.

Security of unpublished ciphers

Commercial packages cracking unpublished encryption schemes built-in:

- MS Word, MS Excel, MS Money
- Word-Perfect, ProWrite, Data Perfect
- Lotus 1-2-3, Symphony, Quattro-Pro
- Paradox, Semantec's Q&A
- PKZip

Time:	1-2 minutes
Price:	~ $200
Companies:	Access Data Crak Software

Passwords recovered even for empty files!

Access Data – DNA: Distributed Network Attack

- client-server application
- DNA client runs in the background, only taking unused processor time
- performs an exhaustive key search on ***Office '97*** and ***Office 2000*** encrypted documents

Expected recovery times (200 MHz, Intel machines):

Product	***Maximum Time***	***Expected***
25 Client Network	16 Days	8 Days
50 Client Network	8 Days	4 Days
100 Client Network	4 Days	2 Days
500 Client Network	20 Hours	10 Hours
1,000 Client Network	10 Hours	5 Hours

Breaking ciphers used in GSM (1)

GSM - world's most widely used mobile telephony system

- 51% market share of all cellular phones, both analog and digital
- over 215 million subscribers in America, Europe, Asia, Africa, and Australia
- In the US, GSM employed in the "Digital PCS" networks of Pacific Bell, Bell South, Omnipoint, etc.

Two voice *encryption algorithms*:

A5/1 and A5/2

encrypt voice between the cellphone and the base station

Breaking ciphers used in GSM (2)

Both voice encryption algorithms

- never published
- designed and analyzed by the secretive "SAGE" group (part of ETSI – European Telecommunications Standard Institute)
- A5/1 believed to be based on the modified French naval cipher

Both algorithms reverse-engineered by
"Marc Briceno" with the Smartcard Developer Association
published by the Berkeley group

A5/1 in May 1999,
A5/2 in August 1999

Breaking ciphers used in GSM (3)

Published attacks

A5/2

August 1999, Ian Goldberg and David Wagner, U.C. Berkeley

Number of operations in the attack ~ $\mathbf{2^{16}}$

A5/1

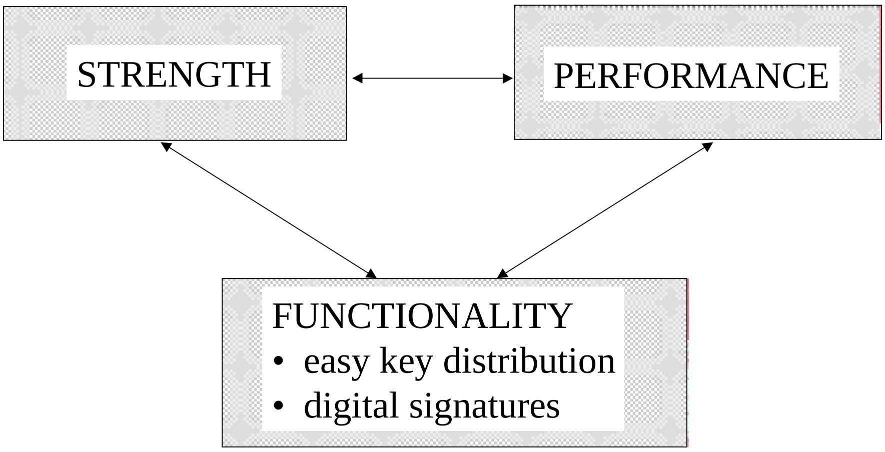
May 1999, Jovan Golic

Number of operations in the attack ~ $\mathbf{2^{40}}$

December 1999, Alex Biryukov and Adi Shamir

Less than **1 second** on a single PC with 128 MB RAM and two 73 GB hard disks.
Based on the analysis of the A5/1 output
during the first two minutes of the conversation.

Features required from today's ciphers

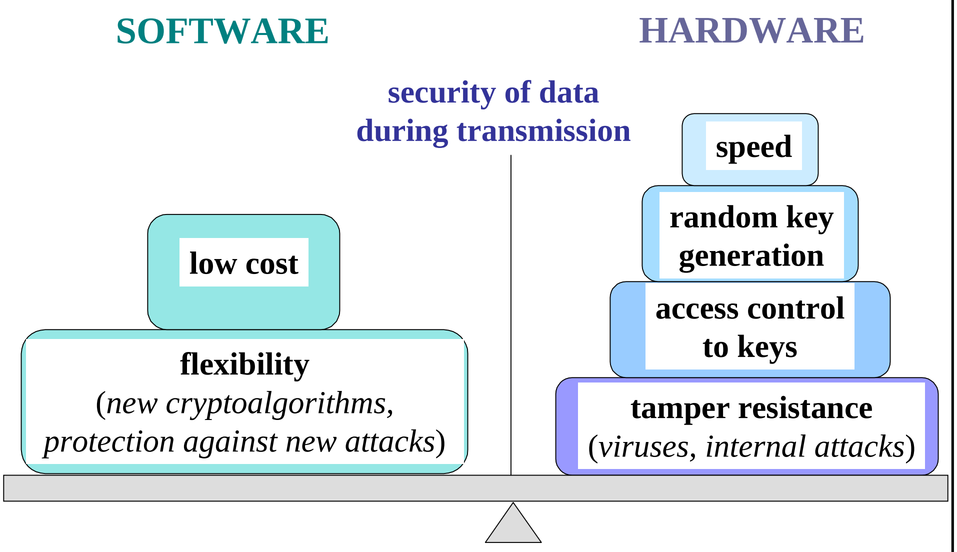


STRENGTH

PERFORMANCE

FUNCTIONALITY
- easy key distribution
- digital signatures

Software or hardware?



SOFTWARE

HARDWARE

security of data
during transmission

low cost

flexibility
(*new cryptoalgorithms, protection against new attacks*)

speed

random key generation

access control to keys

tamper resistance
(*viruses, internal attacks*)

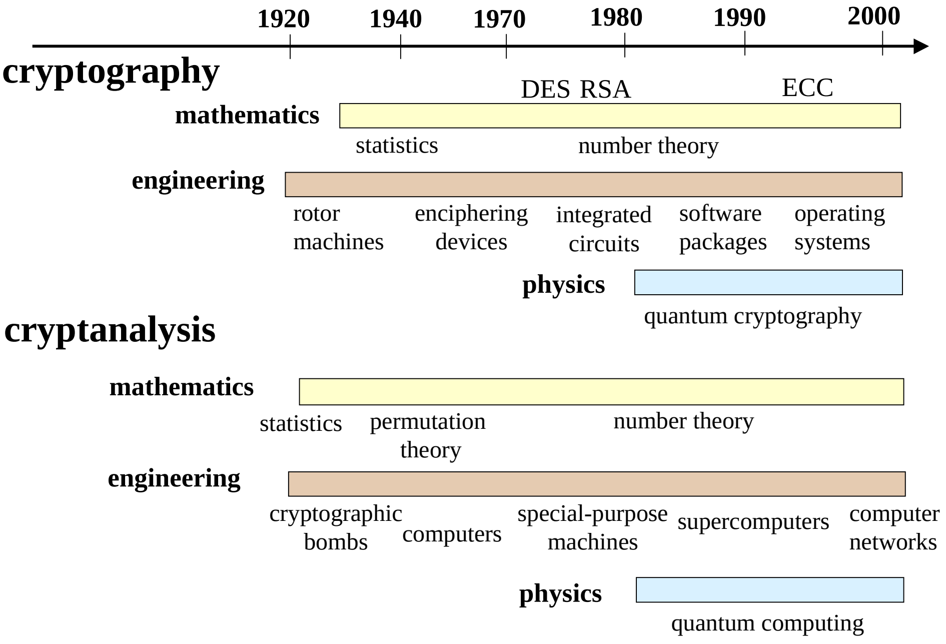
Basic hardware implementations of cryptography

- VLSI chip
- smart card
- PCMCIA card
- cryptographic card
- stand-alone cryptographic device

Applications most suitable for hardware implementations

- hardware accelerators for security gateways and routers
- wireless communications
- universal smart cards for electronic commerce
- electronic wallet
- Certificate Authority - center for registration of public keys
- key-escrow cryptography
- military devices
- high-grade security devices

Evolution of cryptography and cryptanalysis



1920 1940 1970 1980 1990 2000

cryptography

DES RSA ECC

mathematics

statistics number theory

engineering

rotor machines, enciphering devices, integrated circuits, software packages, operating systems

physics

quantum cryptography

cryptanalysis

mathematics

statistics, permutation theory, number theory

engineering

cryptographic bombs, computers, special-purpose machines, supercomputers, computer networks

physics

quantum computing

NSA

National Security Agency
(also known as “No Such Agency”
or “Never Say Anything”)

Created in 1952 by president Truman

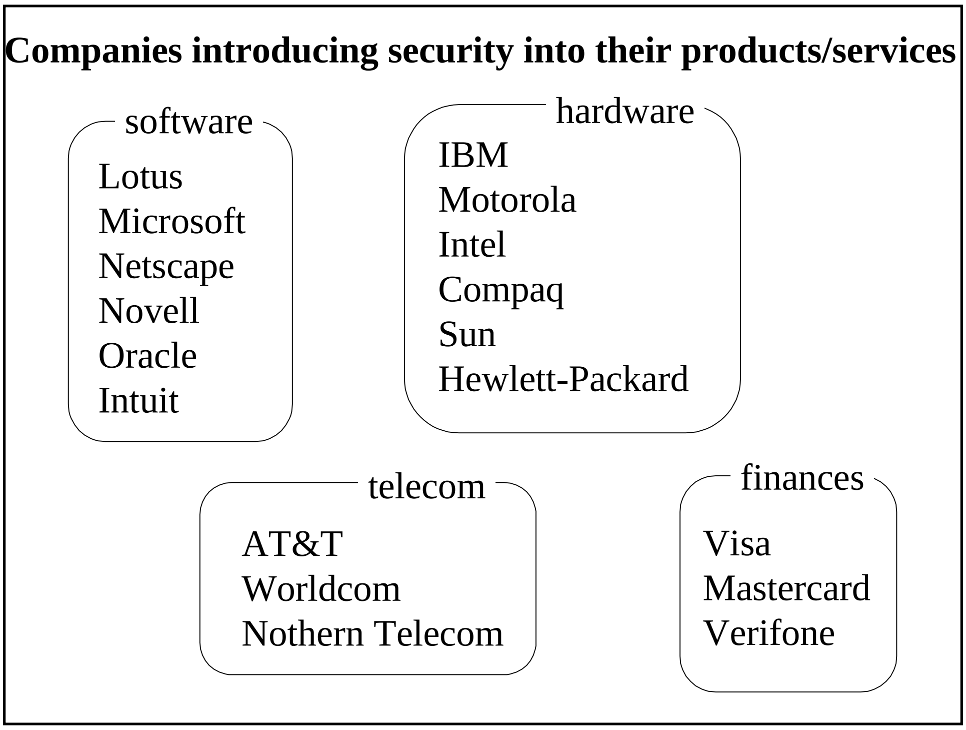
Goals:

- designing strong ciphers (to protect U.S. communications)
- breaking ciphers (to listen to non-U.S. communications)

Budget and number of employees kept secret
Largest employer of mathematicians in the world
Larger purchaser of computer hardware

RSA Security Inc.

- patents for RSA, RC5, RC6 and other cryptographic algorithms
- over 500 mln users of the basic cryptographic library BSAFE
- RSA Laboratory
- RSA Conference
- spin-off companies
  VeriSign - Public Key Infrastructure



Companies introducing security into their products/services

software

Lotus
Microsoft
Netscape
Novell
Oracle
Intuit

hardware

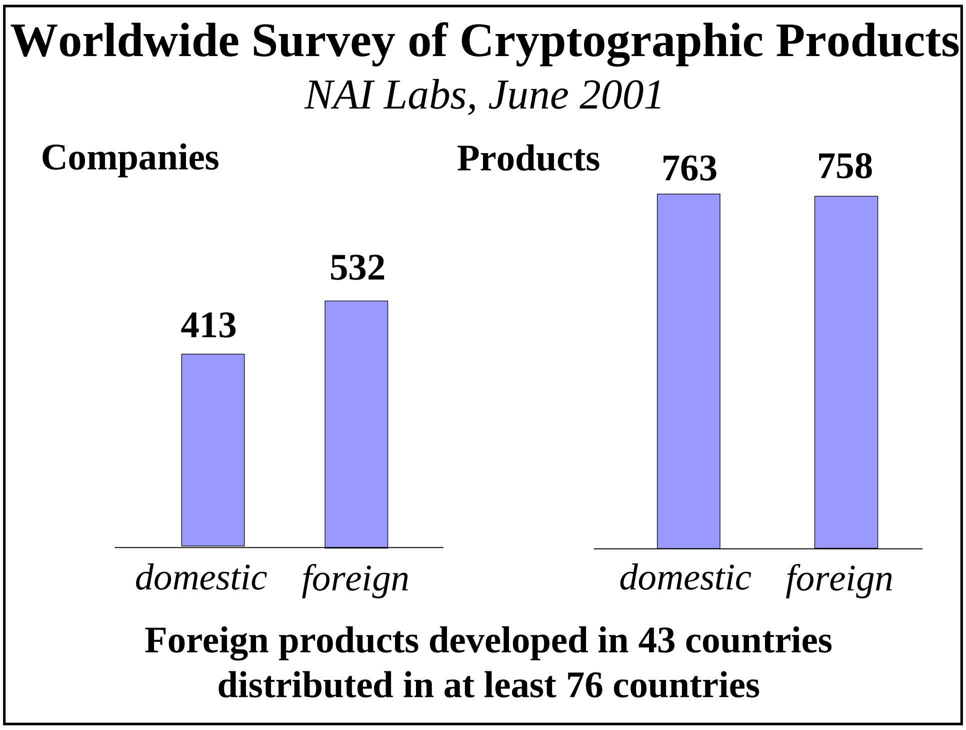
IBM
Motorola
Intel
Compaq
Sun
Hewlett-Packard

telecom

AT&T
Worldcom
Nothern Telecom

finances

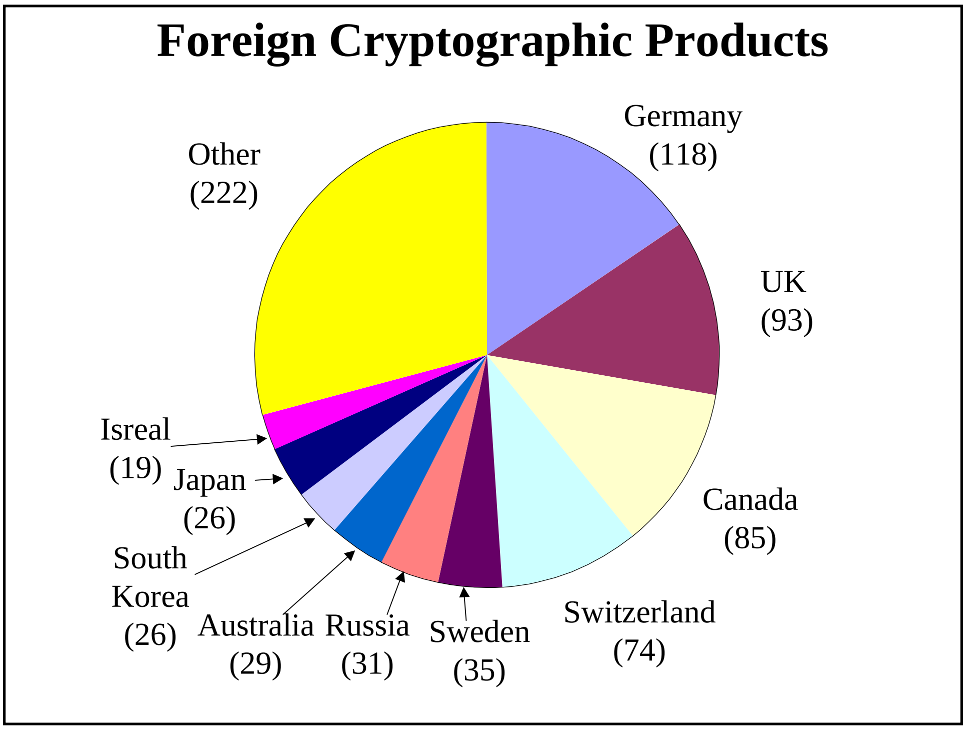
Visa
Mastercard
Verifone



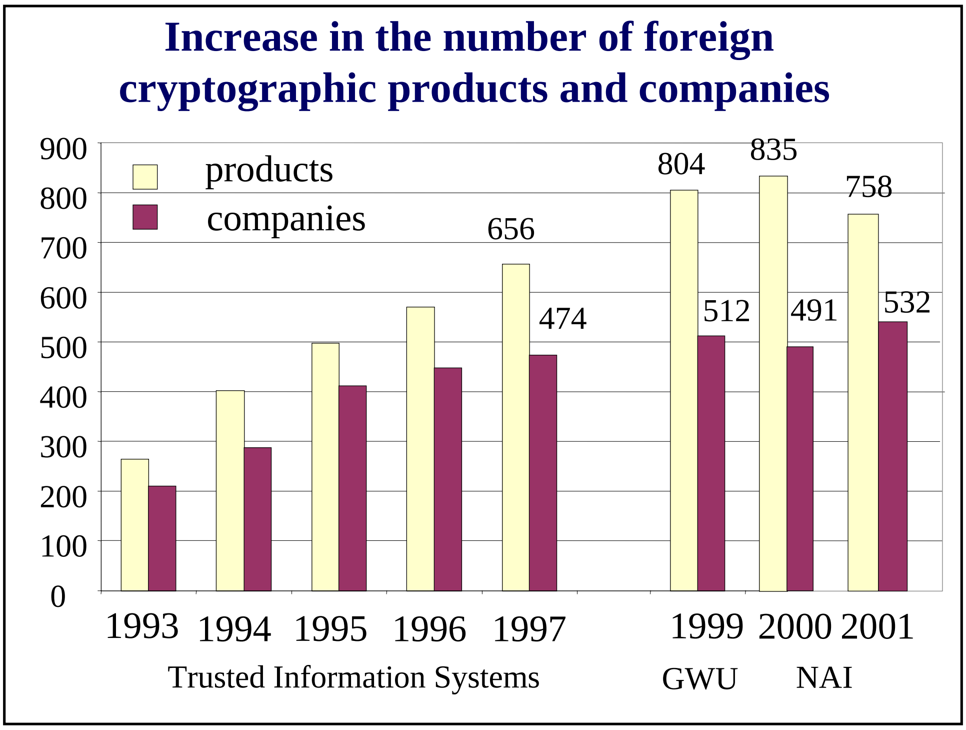
Worldwide Survey of Cryptographic Products

NAI Labs, June 2001

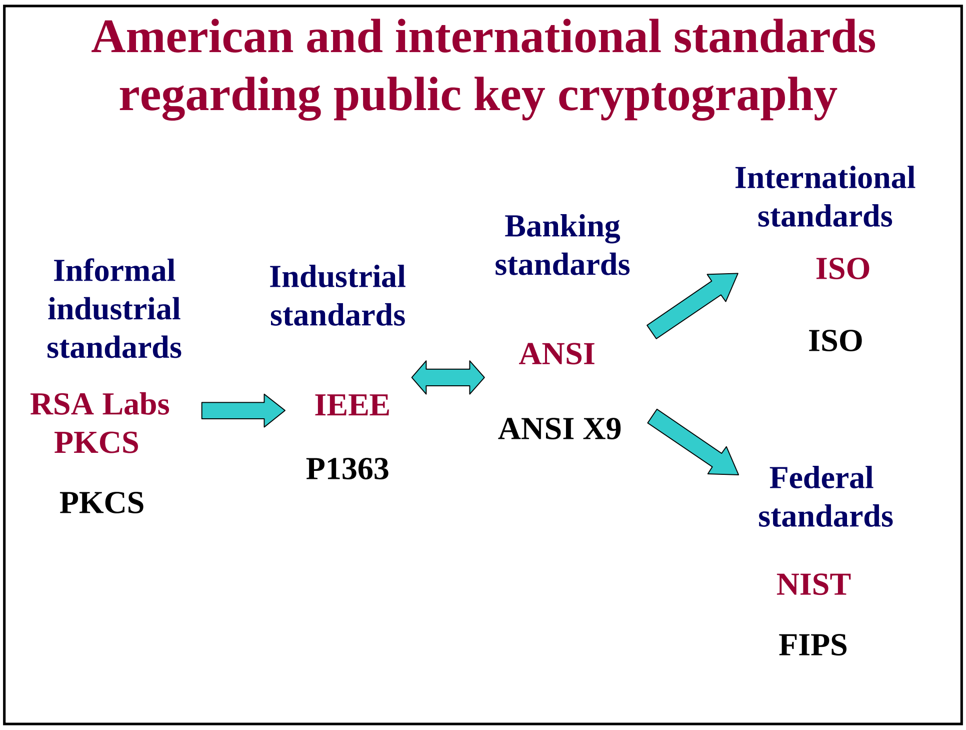
Foreign products developed in 43 countries
distributed in at least 76 countries



Foreign Cryptographic Products



Increase in the number of foreign cryptographic products and companies



American and international standards regarding public key cryptography

Informal industrial standards

RSA Labs PKCS

PKCS

Industrial standards

IEEE

P1363

Banking standards

ANSI

ANSI X9

International standards

ISO

ISO

Federal standards

NIST

FIPS